Association for Information Systems
AIS Electronic Library (AISeL)

Wirtschaftsinformatik Proceedings 2009 | Wirtschaftsinformatik

2009

# IDENTITY MANAGEMENT IN BUSINESS PROCESS MODELLING: A MODEL-DRIVEN APPROACH

Heiko Klarl
*Media Computing, University of Regensburg*

Christian Wolff
*Media Computing, University of Regensburg and iC Consult GmbH*

Christian Emig
*Cooperation & Management, University of Karlsruhe (TH)*

# IDENTITY MANAGEMENT IN BUSINESS PROCESS MODELLING: A MODEL-DRIVEN APPROACH

Heiko Klarl[1,2], Christian Wolff[1], Christian Emig[3]

***Abstract***
*The modelling of business processes is widely used in enterprises. Though this is very common, requirements for identity management and access control are often collected separately in documents or requirement tools. Due to the business-driven background of access control, this kind of requirement should be collected at the business site's business process model. This work introduces a meta-model for modelling access control requirements at the business process level. It combines the model and its requirements, reducing the risk of inconsistencies caused by process changes. A model-driven development process utilises the enriched models for generating policies for different identity management products.*

## 1. Introduction

The success of the internet, the ongoing globalisation and resulting needs for faster communication and interaction with business partners as well as the implementation of new law and business regulations like Basel II or Sarbanes-Oxley Act [6] lead to a demand for new solutions. *Service-oriented architecture* (SOA) tries to cope with those needs: The service-oriented architecture paradigm often uses the modelling of business processes, which is widely used and supported by a variety of well established notations [20, 32, 34] and tools. Despite these facts, (non-functional) requirements which are strongly related to the business process are commonly not integrated in its model. A lot of non-functional requirements arise in the area of *identity management* (IdM) [1], where access control is an important part. Currently, these IdM-related requirements are often "specified" in a non-formalised manner as unstructured text by the business department. If these specifications are not complete and cannot be understood by the IT security department, a complicated and error prone coordination process between both departments arises [cf. 7]. At this time, the application owner – namely the business department – loses its "requirement sovereignty". Therefore it is highly dependent on the support of another department in formulating their own IdM requirements. Such a separation of the business process model and its related IdM requirements may easily result in inconsistencies if changes are not adapted immediately in all specification documents. In the following, we suggest a solution for this problem by enriching the business process model with a specification of IdM requirements. The model is used as the origin of a model-driven software development approach to generate concrete *access control policies* for

1 Media Computing, University of Regensburg, Germany
2 iC Consult GmbH, Keltenring 14, 82041 Oberhaching, Germany
3 Cooperation & Management, University of Karlsruhe (TH), Germany

service-oriented architectures. This work is based on a cooperation project between *iC Consult GmbH*, an independent service provider in the area of identity management, the department of *Media Computing* at the University of Regensburg and the research group *Cooperation and Management* at the University of Karlsruhe. The paper is organised as follows: Section 1 gives a short introduction to identity management and its relation to business process management. In section 2, we introduce our UML2 Profile for IdM as well as the *Web Services Access Control Markup Language* (WSACML), an access control meta-model for service-oriented architecture. Based on both specifications, a model-driven policy development process is described. The application to a real business scenario from the banking domain is shown in section 3. Section 4 discusses related work, and section 5 concludes the paper.

### 1.1. Main Aspects of Identity Management

With the increasing complexity of the IT landscape in enterprises and the penetration of nearly all critical business processes by information technology, identity management is a key factor and one of the main building blocks of IT security [13]. IdM comprises *authentication* of identities, the *authorisation* of resource access as well as the logging of all events relevant for *auditing* requirements. These three pillars of IdM are embedded in several processes in order to mitigate its complexity. Policies containing permissions build the base for access control decisions [27]. They state whether an authenticated subject is allowed to access or interact with an object or a resource within the IT system. In the scope of regulations (e.g. the Sarbanes-Oxley-Act or Basel II), the requirements for the administration and documentation of access permissions and policies lead to a demand for sophisticated IdM solutions. A reference architecture for such a solution is shown in [3]; [17] describes an architecture for IdM in federated environments.

### 1.2. Identity Management and Business Process Modelling

The importance of business processes models became obvious with the idea of business process reengineering [15] in the 90ies and with the upcoming of the service-oriented architecture paradigm [36]. The nearly arbitrary combination of single sub-processes or loosely coupled services to business processes in the sense of service-orientation is only possible on the base of meaningful and executable models. This enables enterprises to cope with market challenges and new business regulations in a flexible and agile way [36]. The focus lies on the optimal support of the business process whereas the IT plays a supporting role in the background. The modelling of business processes can be done in different notations like *Event-driven Process Chains* (EPC) [20], the *Business Process Modeling Notation* (BPMN) [32] or the behaviour diagrams of the *Unified Modeling Language* (UML) [34].

The short lifecycle of business processes and their opening to other businesses in the context of B2B-scenarios requires a constant adoption of IdM requirements in order to reach and guarantee high security standards [21]: On the one hand, functional specifications regarding identities, roles and permissions are constantly changing, on the other hand, changing specifications of the organisational layer, e.g. for supporting privacy or avoiding corruption play an increasing role in enterprise security. In order to meet these demands, traditionally hard coded security mechanisms are replaced by dynamic policies which are changeable at runtime.

Closing the gap between specification of IdM requirements in documents and requirement management tools and the business process' model is still not done, resulting in different complementing specifications [11, 16, 25, 37]. The coupling of the business process' models and its security requirements will ensure a consistent state over all changes – functional ones as well as

those affecting security issues. The management of security relevant aspects will be tied stronger to the business process' development, avoiding inconsistencies in its protection. The business department should be supplied with tools not only for modelling their processes, but also for integrating their IdM requirements in those models.

## 2. Modelling and Transforming IdM Requirements within Business Processes

In order to cope with the problems described above and to force the coupling of business process and its security requirements, we propose the modelling of requirements in business process models. A model-driven approach that generates concrete security policies based on the models will be introduced in the following sections.

### 2.1. The Development Process and its Relation to Model-driven Architecture

The development process typically starts with defining the business process in the business department. Preparatory steps like use-case analyses or textual specifications etc. are not in the focus of this paper: Our contribution starts with the business process already modelled and we see this point as the *computational independent model* (CIM) in the sense of OMGs' *Model-driven Architecture* (MDA) [31]. In this view, the CIM contains all information of the business process – enriched with security specifications based on the UML2 profile for IdM. A semi-automatic transformation process with possible manual additions leads to the *platform independent model* (PIM), containing only security specifications at a platform neutral level. A meta-model for this has been presented as WSACML in [8]. Its generic design does not include any (security) product specific elements, so that the last transformation step can create *platform specific code* (PSC) for different platforms like *CA SiteMinder* or *IBM Tivoli Access Manager*.

### 2.2. Securing a Business Process by the UML2 Profile for Identity Management

The business department should be able to define its own or compliance-driven IdM requirements, using their specific domain knowledge in business process modelling. This enables a fully model-driven software development process, starting with the modelling of IdM requirements in the business department and resulting in security policies for a specific software system.
We utilise UML behaviour diagrams, especially activity diagrams, used for modelling data- and control flows as well as workflows [4, 35]. UML itself is based on a meta-model supported by a variety of tools and known and accepted in enterprises. The UML profile mechanism offers a lightweight approach to extend this meta-model. This can be done by adding new elements for special domains without losing UML's tool support. Stereotypes do not change the meta-model but extend and specify existing UML meta-classes for special use-cases. New elements are named and can immediately be used as the profiles' elements. Constraints are used in order to restrict elements in their behaviour, and can be expressed in prose, (pseudo-) programming languages or in dedicated languages like OCL (*Object Constraint Language*) [33]. Constraints must not be in conflict with inherited constraints of the meta-class. Tagged values are key-value-pairs, enriching stereotypes with additional information. UMLs' syntax and semantic is not touched by UML profile extensions.

The UML2 profile for IdM supports the modelling of access control policies within activity diagrams. In case of a business process it offers the possibility to represent its behaviour as well as its constraints for accessing certain actions. The model of the UML2 profile for IdM is shown in *Figure 1*. The element «IdMAction» extends the UMLs' activity diagram element «action», indicating that this must be secured by the IdM infrastructure. It contains the attributes *complianceClassifier* and *securityClassifier* providing the possibility to classify the element

according to its compliance and security guidelines. Those are defined at the enterprise architectural level. The container element «Policy» links single «Permission» elements in a disjunctive manner; this allows the reuse of «Permission» elements in different «Policy» elements or policies. «Policy» owns the same classification attributes as «IdMAction». In order to avoid conflicts due to contradicting policies as well as to reduce complexity at the business process level, only one policy may be assigned to an «IdMAction». «Permission» elements encapsulate one or more «Assertion» elements for covering one access control situation. The element «Assertion» contains the positive access control statement, allowing access on resources. This means that every access authorisation has to be defined in a dedicated permission. An «Assertion» element aggregates «SubjectAttribute», «ObjectAttribute», «EnvironmentAttribute», «InputParameter» and «Constant».

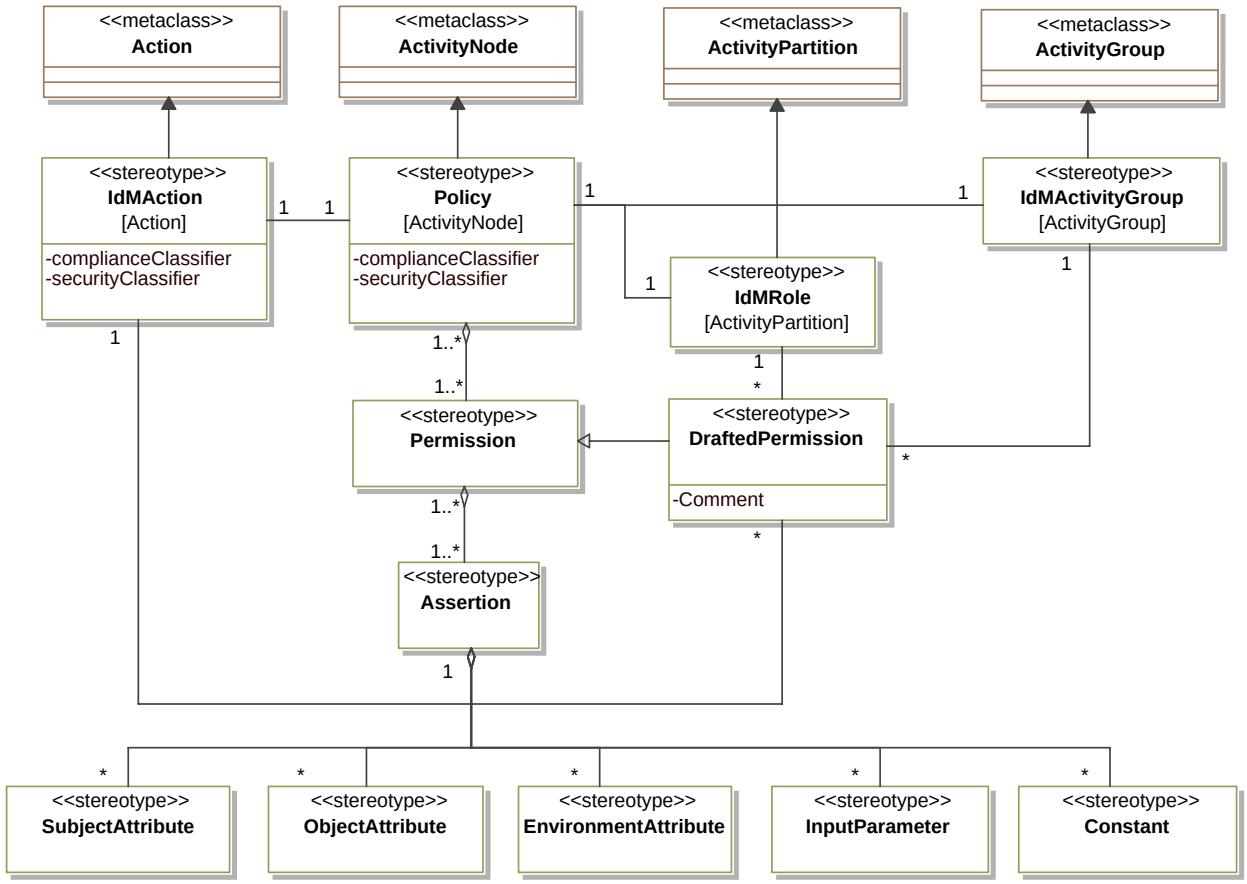


**Figure 1: The UML2 Profile for Identity Management**

The object being accessed is described by the «ObjectAttribute». A sophisticated enterprise architecture with well-defined business objects types supports the selection of relevant object attributes tremendously. «EnvironmentAttribute» contains metadata such as time, date and the systems conditions whereas «InputParameter» specifies input data. For comparing attributes with specific values, «Constant» is used. In case the business department was not able to to properly define an adequate policy with these modelling concepts, a «DraftedPermission» contains access control statements without formalisation, i.e. descriptions of the desired behaviour in prose. These drafts must be refined by business security analysts resulting in a valid set of «Permission» and «Policy» elements. «IdMRole» extends the concept of activity partitions in order to assign business roles to «IdMAction» elements. The same pieces of information can also be covered by utilising «SubjectAttribute» to describe the business role of the accessing subject – which reduces the visual complexity in case of dozens of roles involved in a business process. We consider the description

of roles not in the classical *role-based access control* (RBAC) [10] manner but define a business role as a set of subjects attributes as described in [42]. «IdMActivityGroup» allows grouping of elements for assigning a «Policy» or «DraftedPermission» only once to a set of elements. An overview regarding the elements' constraints defined in the meta-model is given in [22].

### 2.3. WSACML – An Access Control Meta-model for Web Service-Oriented Architecture

Looking at the mass and complexity of the existing and upcoming specifications in the web service security area like WS-Security, WS-Trust, SAML, *eXtensible Access Control Markup Language* (XACML) or the Liberty Alliance's stack proposal [12, 30], it is comprehensible that software developers often neglect the web service security part. Additionally, state-of-the-art IdM suites are not yet prepared for web service-oriented architectures and their accompanying standards [29]. At the same time application servers often do not yet support necessary combinations of relevant IdM standards. This is why currently existing web services in most cases have little or no security features. In [8] we have introduced WSACML, an access control meta-model for web service-oriented architectures which is utilised as meta-model for the platform independent model (PIM). It eases its use, as complexity like in XACML is reduced. WSACML describes policies at the PIM level, which means that they are specified with detailed technical resource descriptions etc. but platform specific details and notations for security products are not covered. This is done by a last transformation shown in detail in [9].

### 2.4. From the Business Process to Concrete Security Policies – The Transformation Process

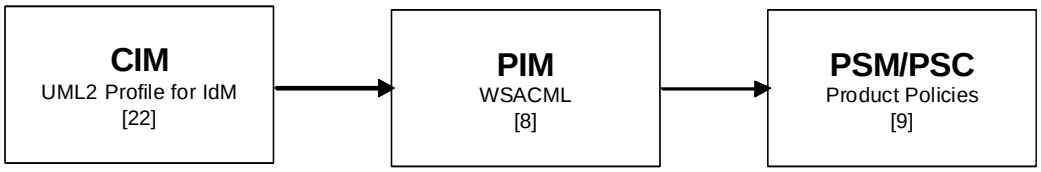


**Figure 2: Overview of Model-driven Policy Development**

In order to create security policies for a certain IdM product, we have implemented a prototypical model-driven transformation process with two transformations (cf. *Figure 2*). To ease the implementation process we utilise a XML-based transformation approach. We generate XML schema definitions (XSDs) based on the meta-models for the CIM and PIM introduced in the previous sections and use them as a template for valid policy information. We start with a business process that has already been modelled and which has been annotated with security policies and extract security-specific information to a XML file (cf. *Listing 1*). In a second step a Java-based application parses this XML-file structured according to the rules of our XSD and transforms the elements according to the mapping rules shown in *Table 1*. Then it checks the compliance with constraints described in [22]. During the transformation process a manual enrichment has to be done by a business security analyst. This analyst should be able to provide additional information for a fine tuning of the security requirements for the platform independent model.

| UML2 Profile for IdM | WSACML |
|---|---|
| IdMAction | Manually resolved to service description and mapped to *ServiceOperationBinding* |
| IdMRole | Builds some parts of the SubjectAttribute |
| IdMActivityGroup | Assignment of the same policy to all IdMActions in this area |
| Policy | Policy |
| DraftedPermission | Empty Policy containing comments, which must be refined by a business security analyst. |
| Permission | Rule |
| Assertion | Assertion |
| *Attribute | *Attribute |
| The * stands for all attributes shown in the meta-model of the UML2 profile for IdM (cf. Figure 1) | |

**Table 1: Mapping rules for the UML2 Profile for IdM to WSACML**

The first transformation process results in a WSACML policy shown in *Listing 2*. Utilising the transformation described in [9], the generation of platform specific code (PSC) comes into play: WSACML policies are transformed into security policies for a certain product. This requires knowledge on the policy-model of the specific security software product. Further information will be provided in [9]. Currently, our transformer tool supports the generation of *CA SiteMinder* policies. A support for *IBM Tivoli Access Manager* is under development at the moment.

```
<SecureBusinessProcess>
  <idmAction complianceClassifier="1"
    securityClassifier="2"
    name="Override Scoring Exception">
    <policyLink
      policyName="Override Scoring Policy" />
  </idmAction>
  <policy name="Override Scoring Policy">
    <permissionLink
      permissionName="ScoringPermission"/>
  </policy>
  <permission name="ScoringPermission">
    <assertion assertionFunction="equal">
      <subjectAttribute value="roleName" />
      <constant value="AM in chief " />
    </assertion>
    <assertion assertionFunction="equal">
      <objectAttribute
        value="exception.type" />
      <constant value="warning" />
    </assertion>
    <assertion assertionFunction="less-than">
      <objectAttribute
        value="exception.score" />
      <constant value="4" />
    </assertion>
  </permission>
</SecureBusinessProcess>
```

**Listing 1: UML2 Profile for IdM (XML representation)**

```
<PolicyContainer>
  <policy name="Override Scoring Exception"
    ruleSelectionAlgorithm="--TODO--"
    serviceOperationBinding
      ="--TODO--Override Scoring Exception">
    <ruleref>ScoringPermission</ruleref>
  </policy>
  <rule name="ScoringPermission">
    <assertion assertionFunction="equal">
      <subjectAttribute value="roleName" />
      <constant value="AM in chief" />" />
    </assertion>
    <assertion assertionFunction="equal">
      <objectAttribute
        value="exception.type" />
      <constant value="warning" />
    </assertion>
    <assertion assertionFunction="less-
     than">
      <objectAttribute
        value="exception.score" />
      <constant value="4" />
    </assertion>
  </rule>
</PolicyContainer>
```

**Listing 2: WSACML**

## 3. Example: Securing a Banking Process

In the banking area business processes are changing often, caused by a very dynamic and customer-driven market environment. As a typical example we choose the opening process for a current account. As the presentation of the complete process might well go beyond the scope of this paper, we show only sections of the process as this should be enough to get an idea of how our method is applied to secure the business process. *Figure 3* shows the business process model with security-

related information added. After a general contract has been created by an account manager the opening of a current account is checked. When the application for a current account is formally correct, a credit rating service is called, followed by a scoring by another service. These actions are secured by the *Check Account Opening Policy*. The policy limits the roles that are allowed to execute those actions to the role 'Account manager' and it may have some contextual restrictions like 'Opening a current account is allowed only at the office times from 7am to 7pm'. If there are no exceptions, the current account will be created; otherwise the opening is delegated to the clerk's supervisor who may override some kind of exceptions (exception score lower than four). This is represented by the *Override Scoring Policy* shown in *Listing 1* which limits the executing role to 'Account manager (AM) in chief' and the exception level lower to four.

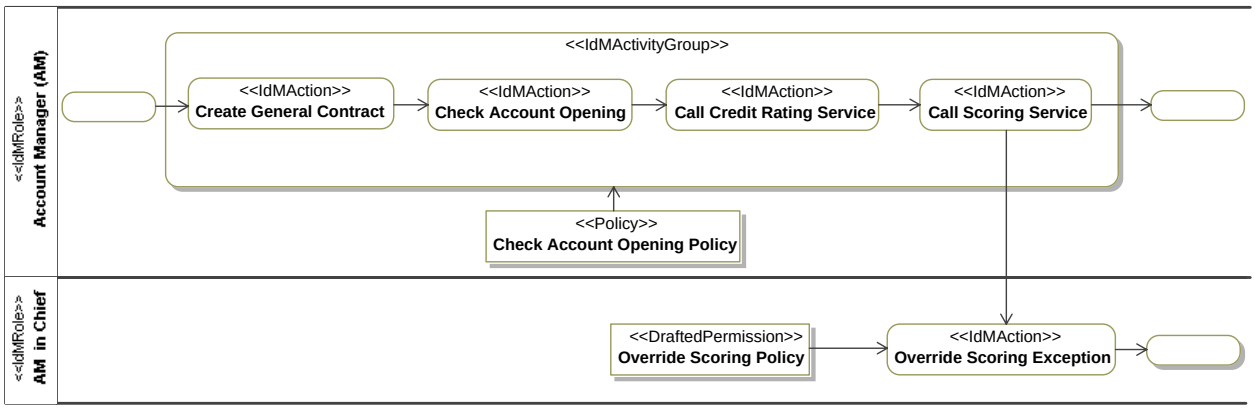


**Figure 2: Secured Business Process Model for Opening a Current Account**

## 4. Related Work

Concerning the integration of requirements in models, many papers have been published recently. The state of the art can be divided into two major parts: On the one hand high level models for usage at business departments, on the other hand IT-centric models like UML class diagrams that are enriched by annotations and requirements. In the area of models for usage at the business site [23] extends the UML activity diagram enabling a modelling of business and performance goals for use with concepts like *balanced score card*. An extension for the UML activity diagram to model *event-driven process chains* (EPC) is shown in [24]. In both papers UML is extended via its profile mechanism.

In the area of information security a meta-model for descriptive collection of requirements is shown in [37, 38]. It is applied to the UML activity diagram via an UML profile as well as to BPMNs' meta-model. Stereotypes like *SecurityAuditing* or *SecurityRequirement* are introduced for usage in the business process model in order to visualise requirements for auditing or the core security requirements like authentication, authorisation and non-repudiation. Nevertheless, most of this work remains at a descriptive level. The stereotypes introduced are just simple annotations comparable with classified comments. In [39] Rodríguez et al. propose the generation of use case views out of business process models which are examined for security requirements. As in their previous work [37, 38], there are no possibilities to specify requirements directly in the business process model and the proposed approach can be only used to find security problems at a high level view. Round trip engineering is missing, so that results found in the use case diagrams can not be added to the processes' model.

In [40] another solution for modelling security goals in BPMN is introduced: A generic security model captures the relations between basic entities like objects, attributes, interactions and effects. The model includes views on the enterprise architectural space which allows connecting elements

from different perspectives. However, it lacks a relationship with the model-driven approach as well as definitions of how policies can be formulated, stored and administrated. In their previous work ([41]) Wolter et al. have proposed an extension of the BPMN for including authorisation constraints which are strongly focused on a *separation of duties* (SoD). Utilising XSLT transformations, the XML representation of the enriched business process is used for generating XACML policies. However, they do not discuss the modelling of *complex* access control scenarios. In contrast to our work, their target model is XACML – this is basically a good idea as it is a standard – but as the application of XACML policies in standard access control products is only partly possible, it would be better to generate concrete policies for certain products.
In the area of workflow security, some further work has been published. In [14] a UML based approach for applying security requirements to the *Web Service Choreography Description Language* (WS-CDL) is proposed. A UML model of the workflow is enriched with security artefacts and could be translated to XML code files that comply with web services standards. As this enrichment is done on a technical level, the procedure will not be viable for the typical business department. Bertino et al. present in [2] how *Web Services Business Process Execution Language* (WS-BPEL) is enriched by authorisation constraints and authorisation information for access control. They introduce the *Business Process Constraint Language* (BPCL) which allows formulating the authorisation constraints. A WS-BPEL engine has been extended to be able to interpret these access control constraints. BPCL is limited to *users*, *roles* and *activities*. Attribute-based access control which we propose as the optimum for service-oriented architecture is not supported. Due to its technical focus, it is not adequate for use at a business department.
Patterns for securing web services are proposed in [18]. The so called *idioms* were applied to orchestrated services and contain technical solutions and templates for predefined threat scenarios. They cover non-functional requirements but only at the orchestration level. An explicit possibility for modelling access control policies or IdM requirements is not given.
Looking at IT-centric research, in [19] an UML profile called UMLsec for modelling safety critical systems is shown. It supports the enrichment of UML class models with security relevant information. Its focus is to support software developers who already are knowledgeable in the security area. The recording of access control policies, especially at the business departments' level is not covered. An UML-based modelling notation combined with a notation for specifying access control models is shown in [26]. This approach is also placed rather late in the software development process, as the requirements are modelled at the class diagrams' level. In [5], Breu et al. propose a model-based development of access policies combining a predicative language (OCL) with XACML as an access policy standard. Access permissions can be specified for methods and method categories at a technical level. A Java-based tool allows the generation of XACML policies. Like other approaches mentioned before, the technical focus of this approach will most likely prevent its application in the context of business departments. Neubauer et al. cover in [28] aspects of secure business processes and its administration. The roadmap of a secure business process is shown in its different stages regarding the inclusion of security aspects. At the second stage he describes the security enriched business process as a base for workflow systems.

Looking at related work, there is on the one hand a very strong focus on business aspects with no possibilities of integrating security requirements. On the other hand the modelling of security requirements is possible on a deeper, workflow or technical level. These solutions often require specialised knowledge of modelling and the architectural aspects of software systems as well as a wide and detailed knowledge on security solutions. Altogether, a gap between modelled business processes at the business departments' site and documents and tools containing the business process' security specifications remains.

## 5. Conclusion

In this paper, we propose a model-driven development process for the creation of access control policies in the context of service-oriented architectures. The development starts with the business process model at the business departments' level, where computational independent process models are enriched with elements for specifying requirements for identity management. Transformation processes translate the model to concrete security policies for different commercial products. The novel aspect of this approach is the direct application of IdM requirements specifications to business process specifications. Thus, the model-driven generation of access control policies can be supported. There is no need for document-based requirement specifications, because all requirements are captured in the business process model where the domain knowledge is available – in the business department. This work lays the fundament by proposing how access control policies can be specified in business processes. Future work will be done on improving the graphical modelling of the business process and its security requirements. The business department will be supported by easy to handle tools, with optimised usability for modelling security enriched business processes. The modelling process will be complemented by utilising policy and business objects repositories to benefit from (re)using existing data. Another aspect being worked on will be the checking of secured business process models for being in compliance with the enterprise's security standards or law regulations.

## 6. References


[1] H. Bagheri and S.-H. Mirian-Hosseinabadi. Injecting security as aspectable NFR into software architecture. In *Proc. 14th Asia-Pacific Software Engineering Conf.*, pages 310–317. IEEE Computer Society, 2007.

[2] E. Bertino, J. Crampton, and F. Paci. Access Control and Authorization Constraints for WS-BPEL. In *IEEE Int'l Conf. on Web Services*, pages 275–284. IEEE Computer Society, 2006.

[3] D. Blum. Identity Management. Technical report, Burton Group, Nov. 2005.

[4] M. Born, E. Holz, and O. Kath. *Softwareentwicklung mit UML 2*. Addison-Wesley, München, 2004.

[5] R. Breu, G. Popp, and M. Alam. Model based development of access policies. *International Journal on Software Tools for Technology Transfer*, 9(5–6):457–470, Oct. 2007.

[6] M. Burling. The key to compliance. *Database-and-Network-Journal*, 35(3):17–18, 2005.

[7] S. Cormack, A. Cater-Steel, J. H. Nord, and G. D. Nord. Resolving the troubled IT-business relationship from a cultural perspective. In *Proc. 12th Australasian Conf. on Information Systems*, Australia, Dec. 2001.

[8] C. Emig, F. Brandt, S. Abeck, J. Biermann, and H. Klarl. An Access Control Metamodel for Web Service-Oriented Architecture. In *Proc. Int'l Conf. Software Engineering Advances*. IEEE Computer Society, Aug. 2007.

[9] C. Emig, S. Kreuzer, S. Abeck, J. Biermann, and H. Klarl. Model-Driven Development of Access Control Policies for Web Services, In *IASTED Int'l. Conf. on Software Engineering and Applications*, Florida, 2008

[10] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli. Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security*, 4(3):224–274, Aug. 2001.

[11] D. Firesmith. Engineering Security Requirements. *Journal of Object Technology*, 2(1):53–68, 2003.

[12] C. Gutiérrez, E. Fernández-Medina, and M. Piattini. A Survey of Web Services Security. In *Computational Science and Its Applications - ICCSA 2004*, volume 3043 of *LNCS*, pages 968–977. Springer, Apr. 2004.

[13] S. Götzfried. Identity Management. Untersuchungen zum Einsatz von Identity Management-Systemen in Unternehmen und Organisationen. Master's thesis, Univ. Regensburg, Informationswissenschaft, 2007.

[14] M. Hafner and R. Breu. Realizing Model Driven Security for Inter-organizational Workflows with WS-CDL and UML 2.0. In *Model Driven Engineering Languages and Systems*, volume 3713 of *LNCS*, pages 39–53. Springer, 2005.

[15] M. Hammer. Reengineering work: don´t automate, obliterate. *Harvard Business Review*, 68(4):104–112, 1990.

[16] G. Herrmann and G. Pernul. Viewing business-process security from different perspectives. *International Journal of Electronic Commerce*, 3(3):89–103, 1999.

[17] W. Hommel. *Architektur- und Werkzeugkonzepte für föderiertes Identitäts-Management*. PhD thesis, Fakultät für Mathematik, Informatik und Statistik der Ludwig-Maximilians-Universität München, 2007.
[18] T. Imamura and M. Tatsubori. Patterns for Securing Web Services Messaging. In *OPSLA Workshop on Web Services and Service Oriented Architecture Best Practice and Patterns*, 2003.
[19] J. Juerjens. *Secure Systems Development with UML*. Springer, 2005.
[20] G. Keller, M. Nüttgens, and A.-W. Scheer. *Semantische Prozessmodellierung auf der Grundlage Ereignisgesteuerter Prozessketten (EPK)*, volume 89. Universität des Saarlandes, Jan. 1992.
[21] H. Klarl. Modellgetriebene, mustergestützte Sicherheit in serviceorientierten Architekturen. *Informatik-Spektrum*, 30(3):175–177, June 2007.
[22] H. Klarl, C. Wolff, and C. Emig. Abbildung von Zugriffskontrollaussagen in Geschäftsprozessmodellen. In *Modellierung 2008 – Verhaltensmodellierung: Best Practices und neue Erkenntnisse*, Berlin, Mar. 2008.
[23] B. Korherr and B. List. Extending the UML 2 Activity Diagram with Business Process Goals and Performance Measures and the Mapping to BPEL. In *Advances in Conceptual Modeling - Theory and Practice*, volume 4231 of *LNCS*, pages 7–18. Springer, 2006.
[24] B. Korherr and B. List. A UML 2 Profile for Event Driven Process Chains. In *Research and Practical Issues of Enterprise Information Systems*, volume 205 of *IFIP International Federation for Information Processing*, pages 161–172. Springer, 2006.
[25] M. N. Kreeger and I. Duncan. Engineering secure software by modelling privacy and security requirements. In *39th Int'l Carnahan Conf. on Security Technology*, pages 37–40, Oct. 2005.
[26] T. Lodderstedt, D. A. Basin, and J. Doser. SecureUML: A UML-Based Modeling Language for Model-Driven Security. *The Unified Modeling Language*, volume 2460 of *LNCS*, pages 426–441. Springer, 2002.
[27] A. Matheus. How to Declare Access Control Policies for XML Structured Information Objects using OASIS' eXtensible Access Control Markup Language (XACML). In *Proc. 38th Annual Hawaii Int'l Conf. on System Sciences*, page 168a. IEEE Computer Society, 2005.
[28] T. Neubauer, M. Klemen, and S. Biffl. Secure Business Process Management: A Roadmap. In *Proc. First Int'l Conf. on Availability, Reliability and Security*, pages 457 – 464. IEEE Computer Society, Apr. 2006.
[29] M. Neuenschwander. Enterprise Identity Management Market 2006–2007. Burton Group, Nov. 2006.
[30] H. R. M. Nezhad, B. Benatallah, F. Casati, and F. Toumani. Web Services Interoperability Specifications. *Computer*, 39(5):24–32, 2006.
[31] Object Management Group, Inc. Model Driven Architecture (MDA). `http://www.omg.org/cgi-bin/apps/doc?ormsc/01-07-01.pdf`, July 2001.
[32] Object Management Group, Inc. Business Process Modeling Notation (BPMN) Specification. `http://www.bpmn.org/Documents/OMG Final Adopted BPMN 1-0 Spec 06-02-01.pdf`, 2006.
[33] Object Management Group, Inc. Object Constraint Language – Version 2.0. `http://www.omg.org/technology/documents/formal/ocl.htm`, May 2006.
[34] Object Management Group, Inc. Unified Modeling Language: Infrastructure – Version 2.1.1. `http://www.omg.org/docs/formal/07-02-06.pdf`, Feb. 2007.
[35] Object Management Group, Inc. Unified Modeling Language: Superstructure – Version 2.1.1. `http://www.omg.org/docs/formal/07-02-05.pdf`, Feb. 2007.
[36] J.-P. Richter, H. Haller, and P. Schrey. Serviceorientierte Architektur. *Informatik-Spektrum*, 28(5):413–416, Oct. 2005.
[37] A. Rodríguez, E. Fernández-Medina, and M. Piattini. Security Requirement with a UML 2.0 Profile. In *Proc. First Int'l Conf. on Availability, Reliability and Security*, pages 670–677. IEEE Computer Society, 2006.
[38] A. Rodríguez, E. Fernández-Medina, and M. Piattini. A BPMN Extension for the Modeling of Security Requirements in Business Processes. *IEICE-Transactions on Info and Systems*, E90-D(4):745–752, 2007.
[39] A. Rodríguez, E. Fernández-Medina, and M. Piattini. Towards CIM to PIM Transformation: From Secure Business Processes Defined in BPMN to Use-Cases. In *Business Process Management*, volume 4714 of *LNCS*, pages 408–415. Springer, Sept. 2007.
[40] C. Wolter, M. Menzel, and C. Meinel. Modelling Security Goals in Business Processes. In *Modellierung 2008*, volume P-127 of *LNI*, pages 201–216, Bonn, Germany, Mar. 2008. Köllen.
[41] C. Wolter, A. Schaad, and C. Meinel. Deriving XACML Policies from Business Process Models. In *Web Information Systems Engineering*, volume 4832 of *LNCS*, pages 142–153. Springer, 2007.
[42] E. Yuan and J. Tong. Attributed based access control (ABAC) for Web services. In *Proc. IEEE Int'l Conf. on Web Services*. IEEE Computer Society, July 2005.
All web references were checked on 28th July 2008.